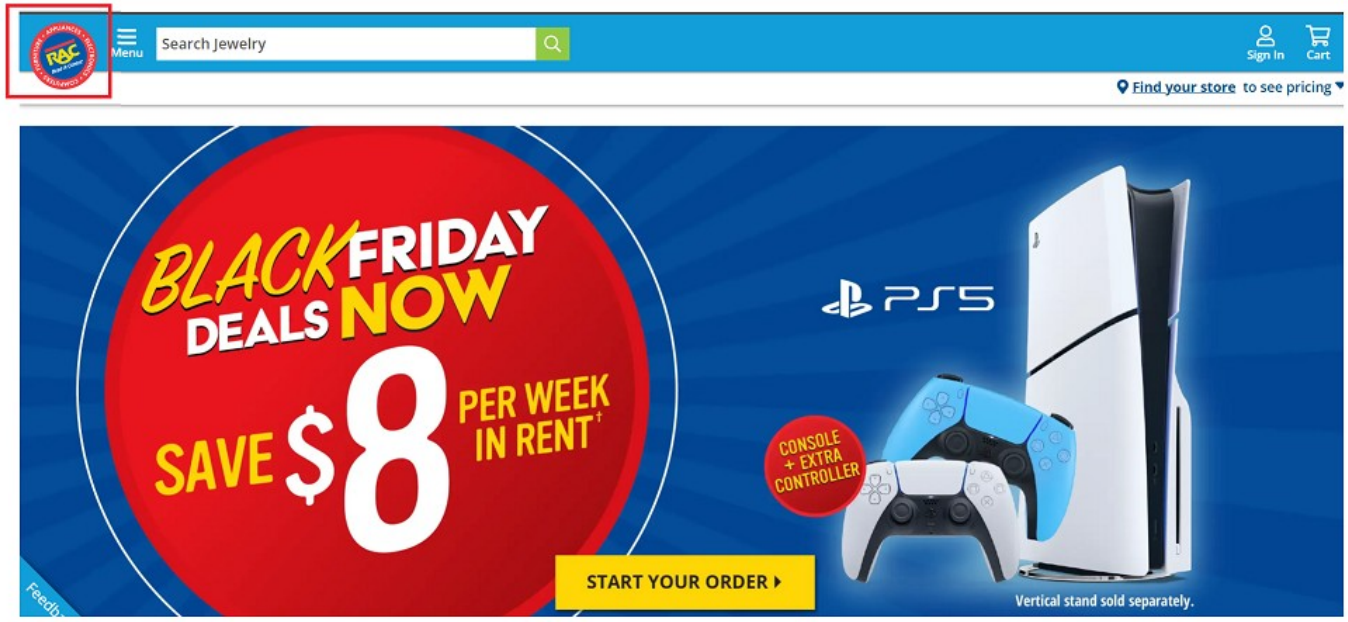
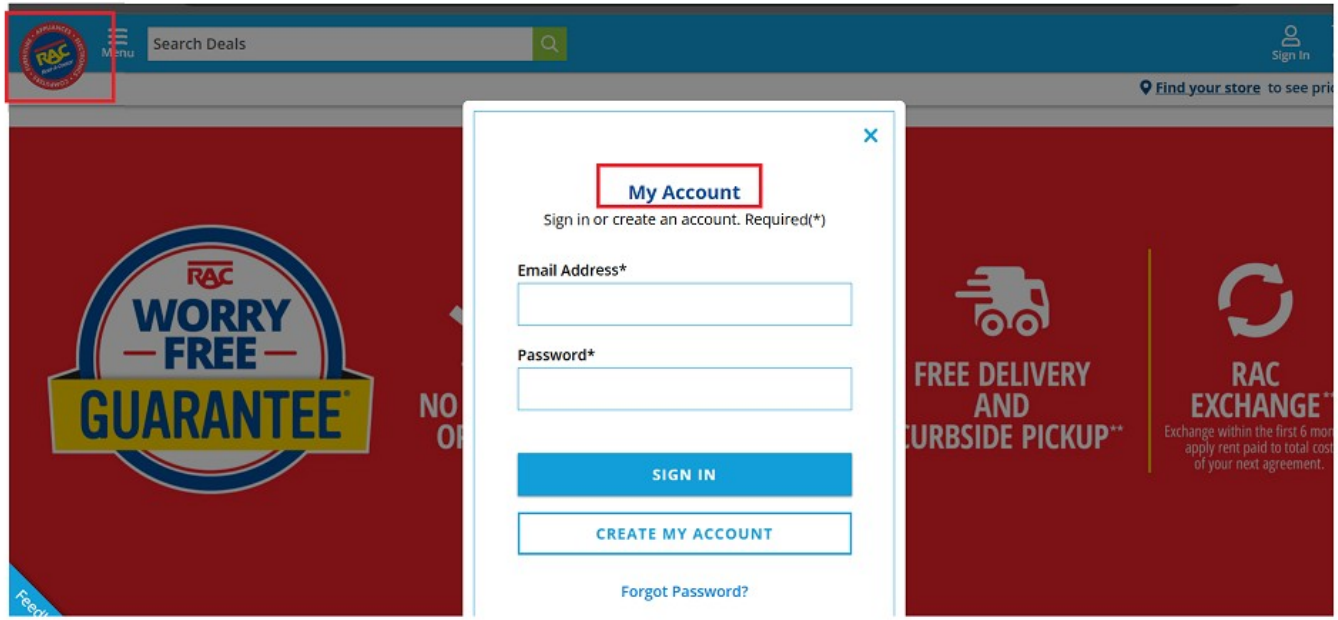
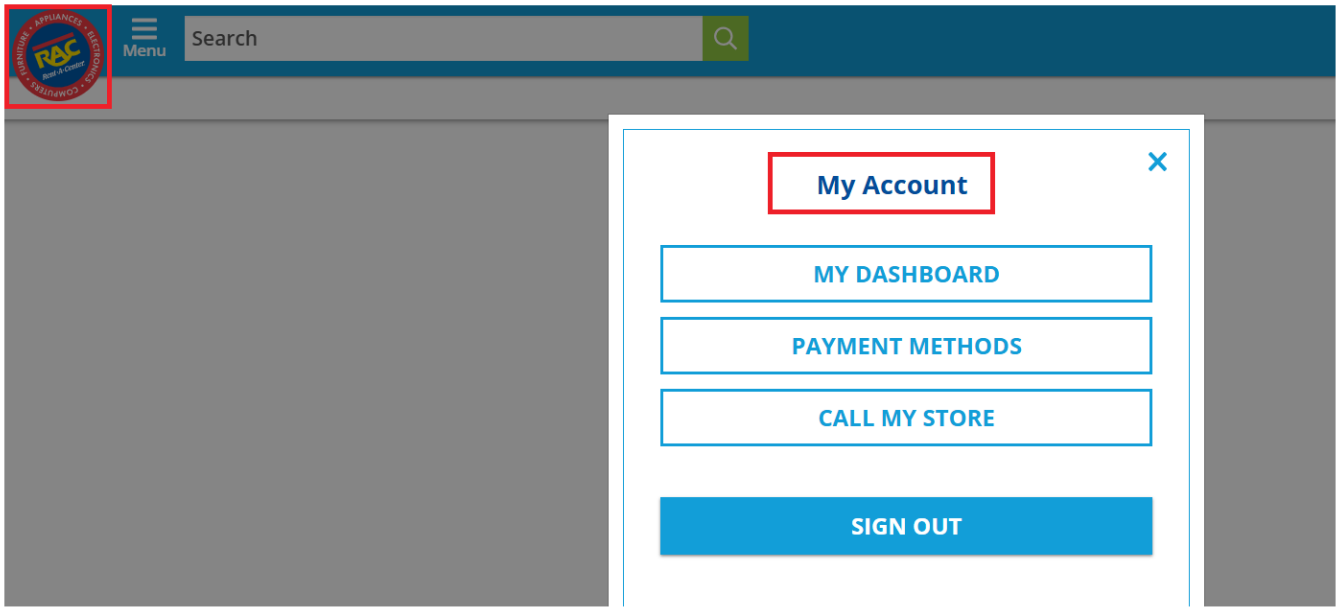
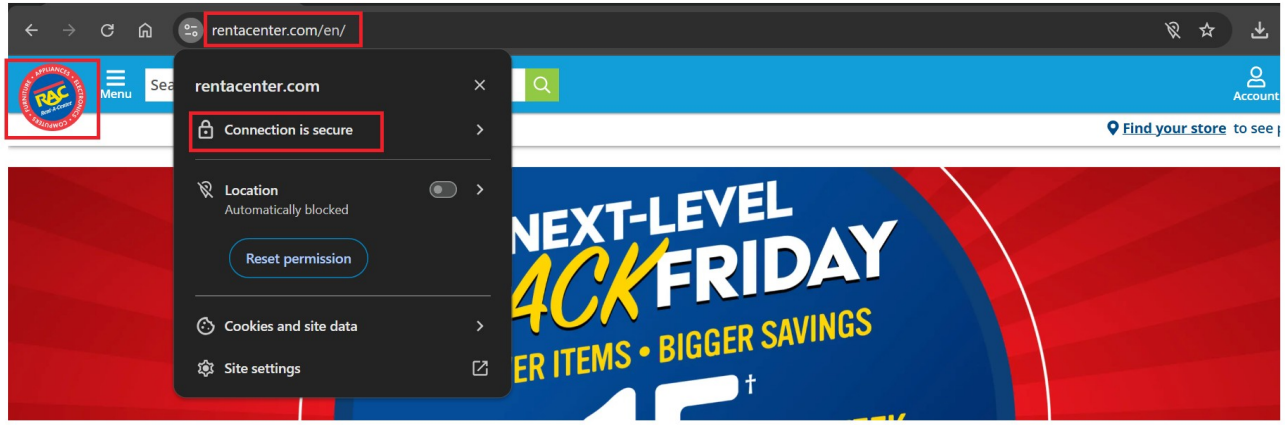
Exhibit 2

US8677116B1	Rent-A-Center, Inc's website "rentacenter.com" ("The accused instrumentality")
1. A method of using a computer system to authenticate a user seeking to conduct at least one interaction with a secured capability provided by a computer, the method comprising:	The accused instrumentality practices a method of using a computer system (e.g., authentication server of the accused instrumentality, etc.) to authenticate a user seeking to conduct at least one interaction (e.g., account login, etc.) with a secured capability provided by a computer (e.g., server of the accused instrumentality). As shown, the website of the accused instrumentality practices providing secure connection with a user's device (electronic device of the user) through HTTPS connections. This is achieved by an authentication server (a computer system) authenticating users seeking to perform actions such as account login, etc., (interactions) ensuring that interactions with secured features are protected from unauthorized access.  https://www.rentacenter.com/

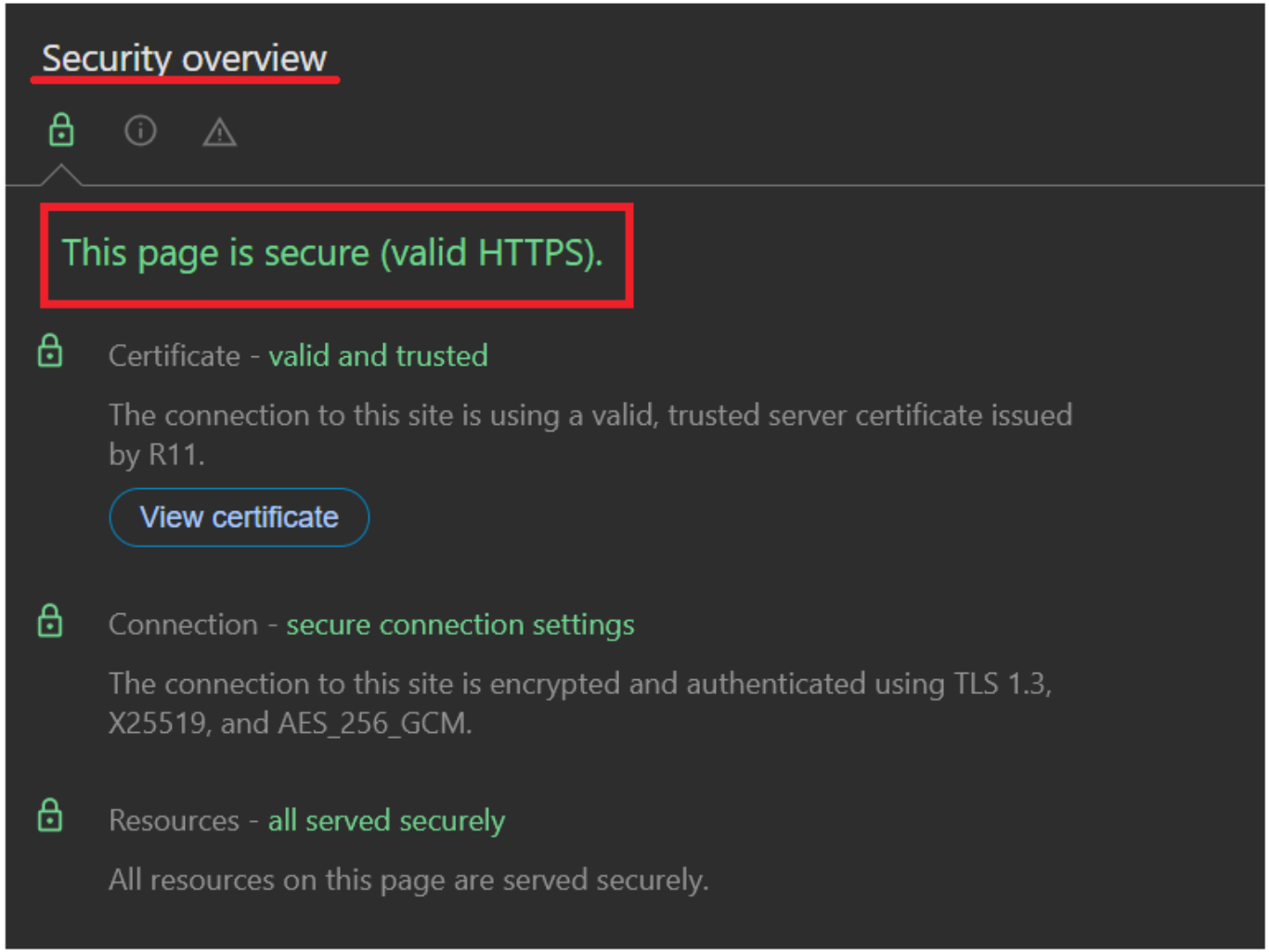
	 https://www.rentacenter.com/en/



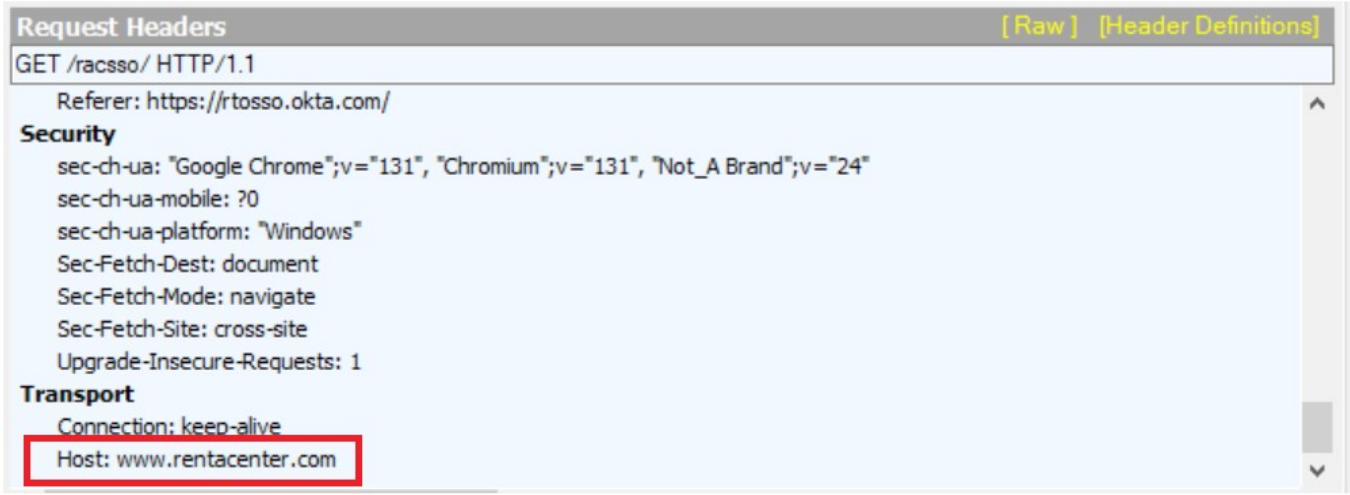
https://www.rentacenter.com/en/



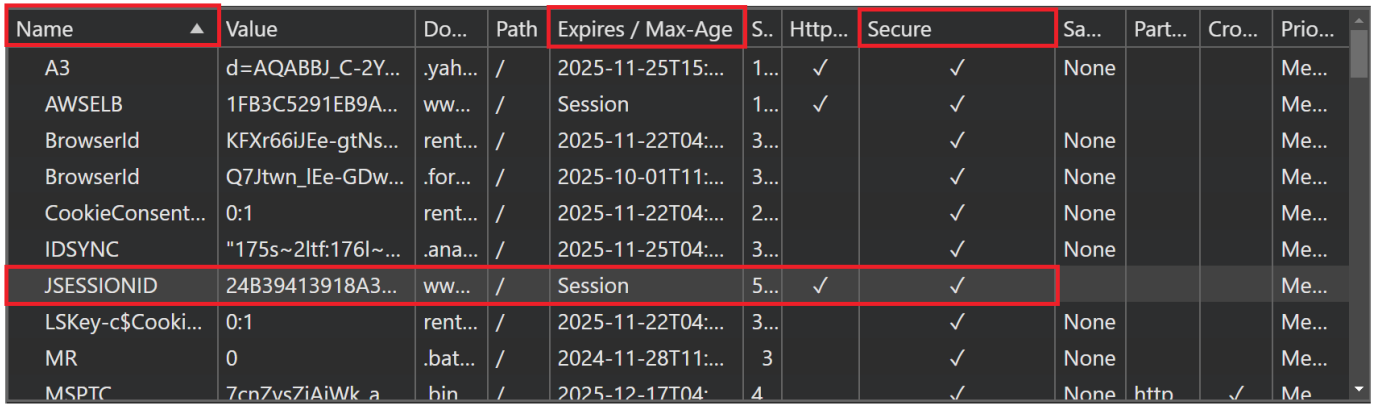
https://www.rentacenter.com/en/



https://www.rentacenter.com/en/



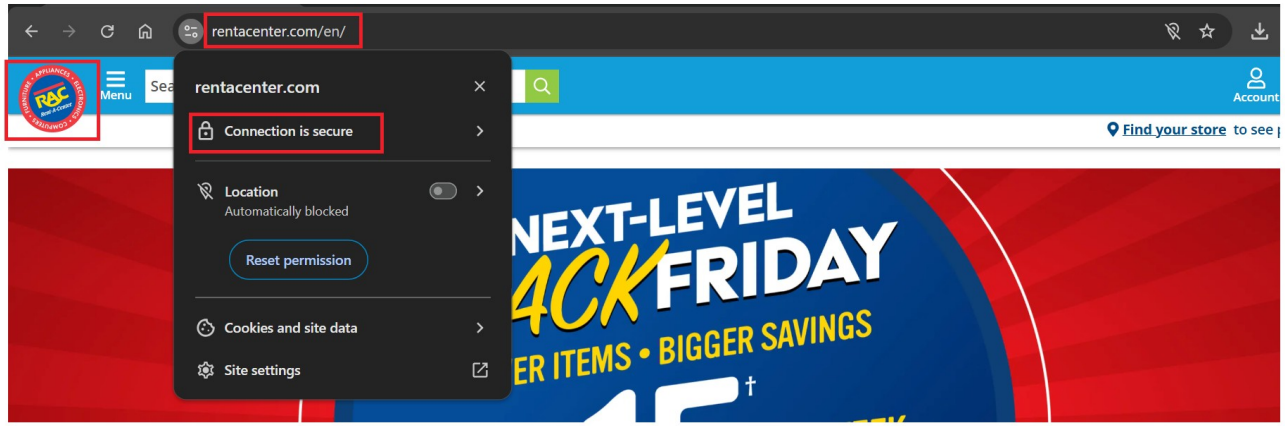
Source: Fiddler capture of the accused instrumentality

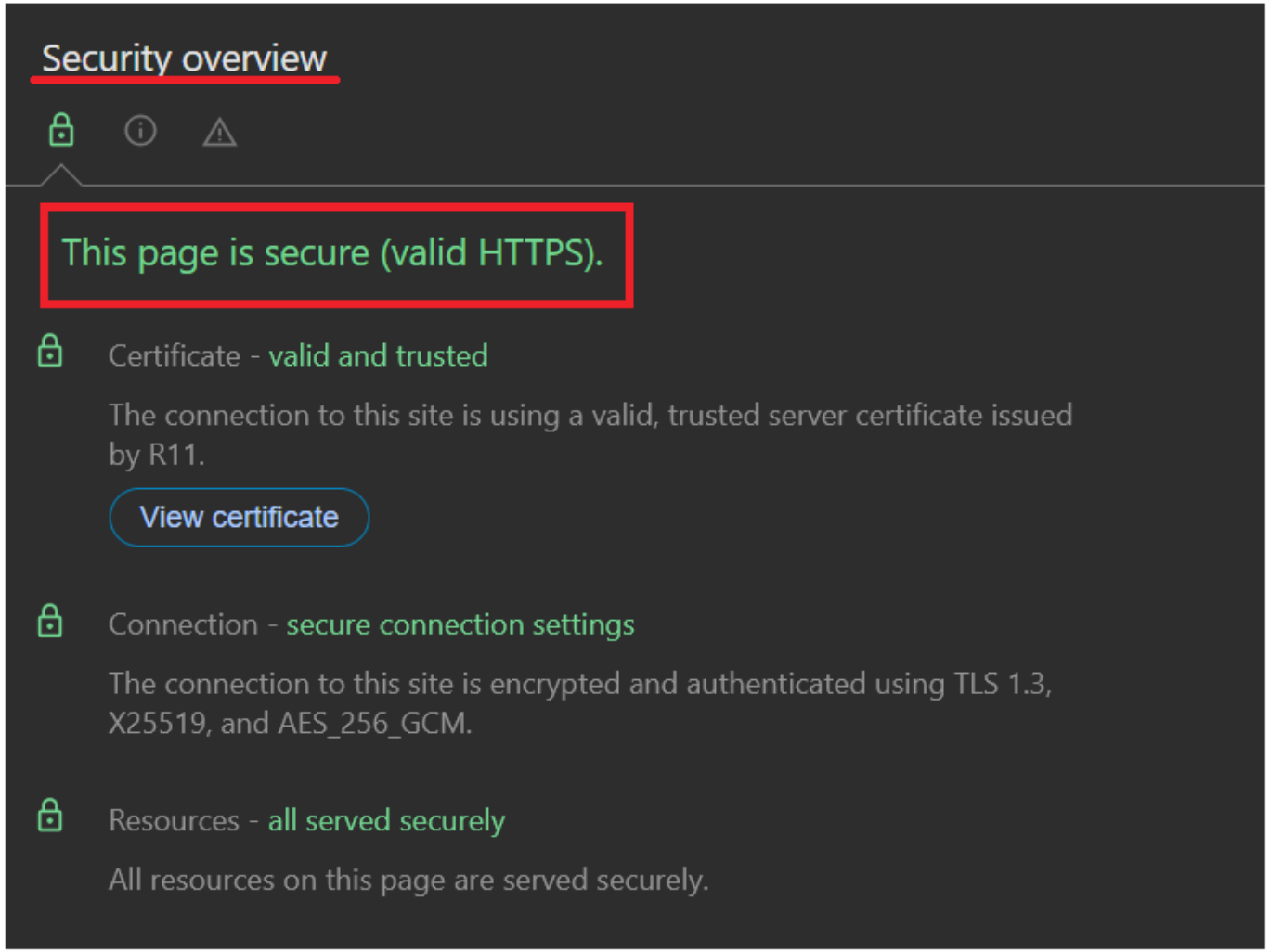


Name	Value	Do...	Path	Expires / Max-Age	S..	Http...	Secure	Sa...	Part...	Cro...	Prio...
A3	d=AQABBJ_C-2Y...	.yah...	/	2025-11-25T15:...	1...	✓	✓	None			Me...
AWSELB	1FB3C5291EB9A...	ww...	/	Session	1...	✓	✓				Me...
BrowserId	KFXr66iJEe-gtNs...	rent...	/	2025-11-22T04:...	3...		✓	None			Me...
BrowserId	Q7Jtwn_lEe-GDw...	.for...	/	2025-10-01T11:...	3...		✓	None			Me...
CookieConsent...	0:1	rent...	/	2025-11-22T04:...	2...		✓	None			Me...
IDSYNC	"175s~2ltf:176l~...	.ana...	/	2025-11-25T04:...	3...		✓	None			Me...
JSESSIONID	24B39413918A3...	ww...	/	Session	5...	✓	✓				Me...
LSKey-c$Cooki...	0:1	rent...	/	2025-11-22T04:...	3...		✓	None			Me...
MR	0	.bat...	/	2024-11-28T11:...	3		✓	None			Me...
MSPTC	7cnZvsZiAiWk_a	.bin	/	2025-12-17T04:	4		✓	None	http	✓	Me

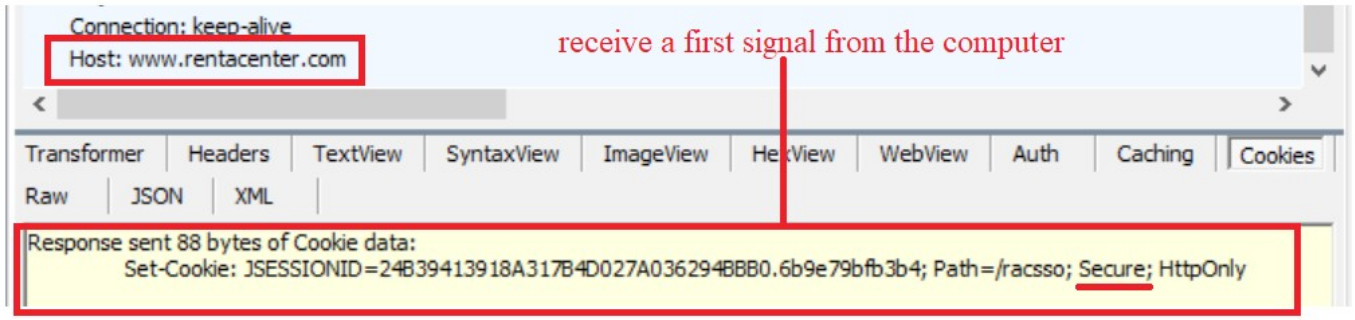
https://www.rentacenter.com/en/

using the computer system to receive a first signal from	The accused instrumentality practices using the computer system (e.g., authentication server of the accused instrumentality, etc.) to receive a first signal (e.g., a JSESSIONID set

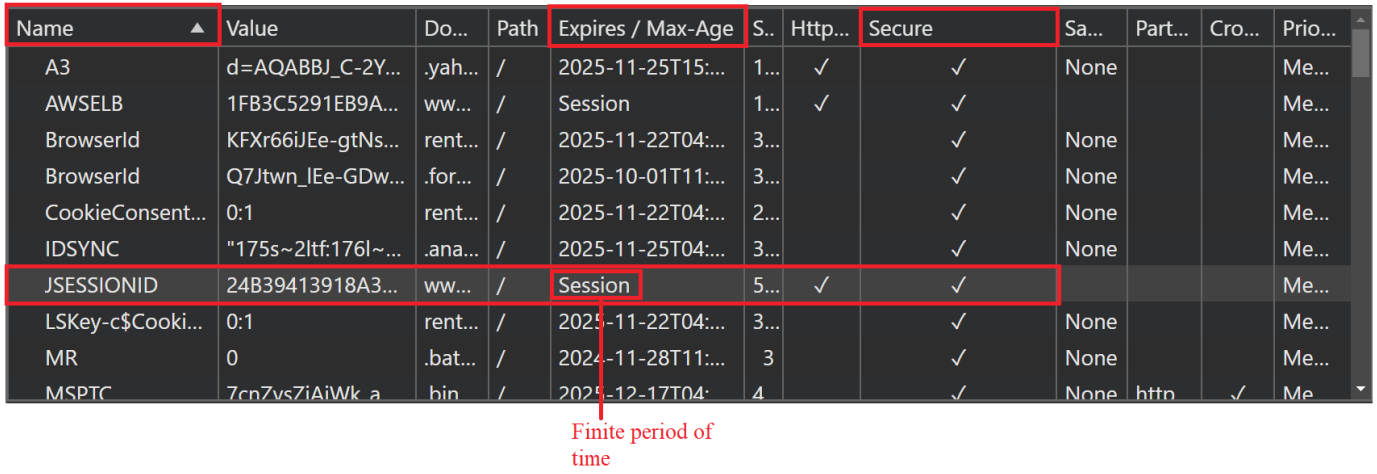
the computer providing the secured capability, the first signal comprising a reusable identifier corresponding to the secured capability, the reusable identifier assigned for use by the secured capability for a finite period of time;	response, etc.) from the computer (e.g., server of the accused instrumentality) providing the secured capability (e.g., secure connection with the website, etc.), the first signal comprising a reusable identifier (e.g., JSESSIONID, etc.) corresponding to the secured capability (e.g., secure connection with the website, etc.), the reusable identifier assigned for use by the secured capability for a finite period of time (e.g., Max-Age). As shown, the website of the accused instrumentality practices providing secure connection with a user's device (electronic device of the user) through HTTPS connections. This is achieved by an authentication server (a computer system) authenticating users seeking to perform actions such as account login, etc., (interactions) ensuring that interactions with secured features are protected from unauthorized access. The server sends a response to set JSESSIONID value, which is set by the user device. As shown, the JSESSIONID token set by the end device is reused in all further communications with the server. The JSESSIONID token also mentions a Max-Age for the token, indicating that it can be reused for a finite period.  https://www.rentacenter.com/en/



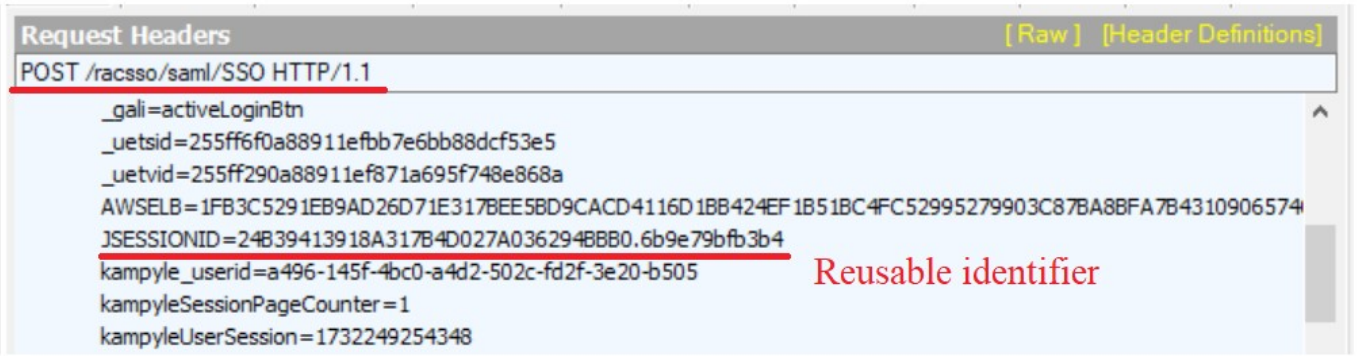
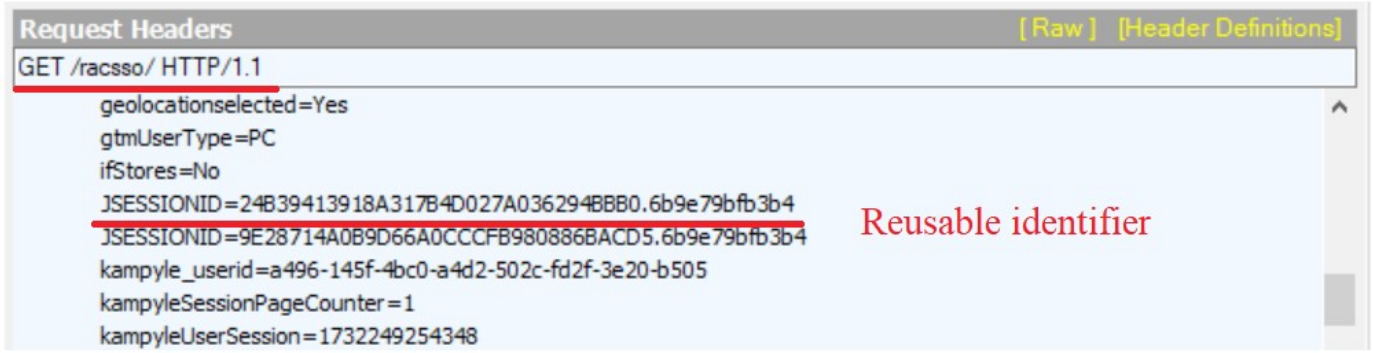
https://www.rentacenter.com/en/

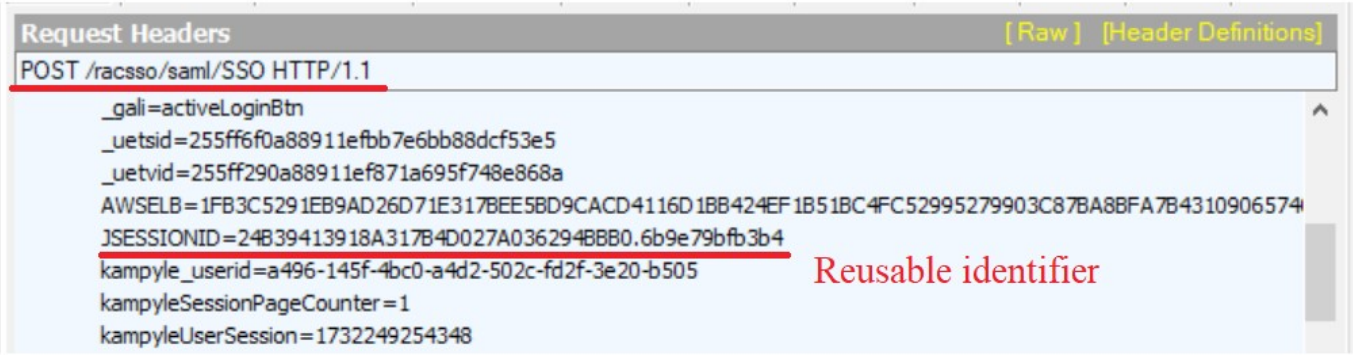
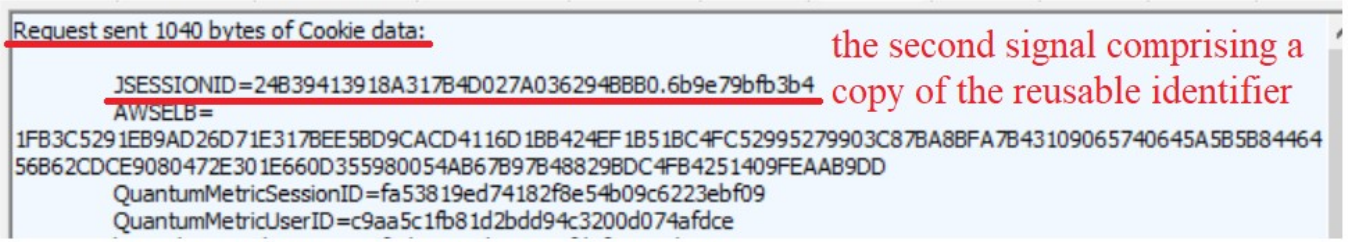


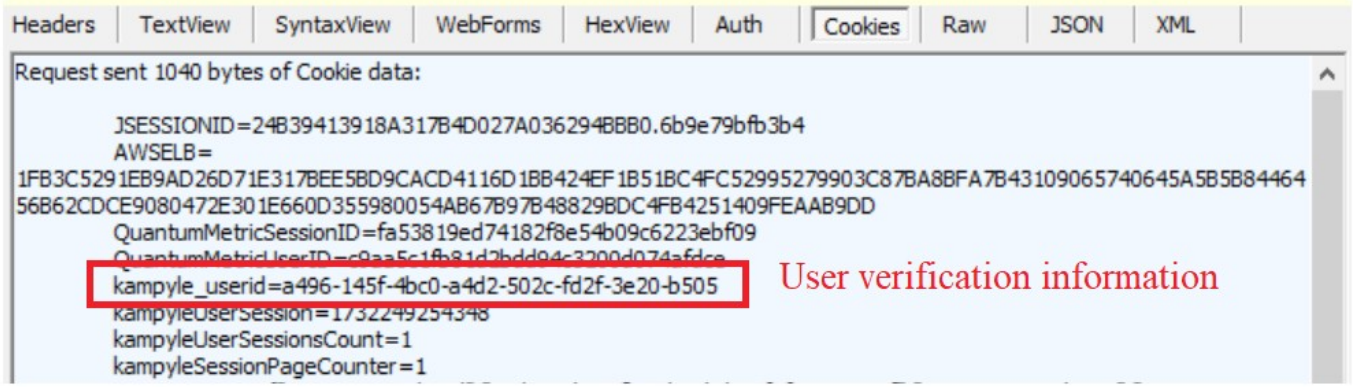
Source: Fiddler captures of the accused instrumentality

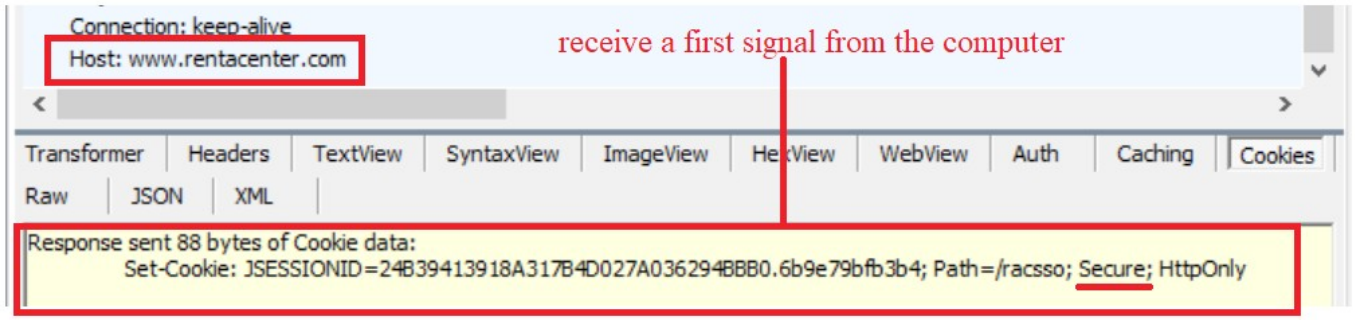


https://www.rentacenter.com/en/

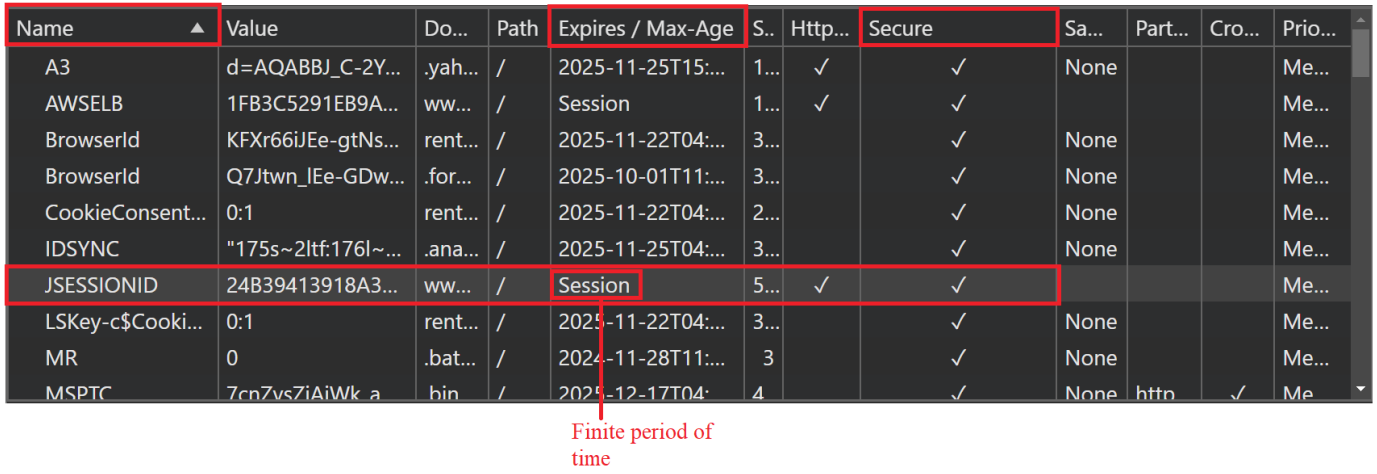
	 Source: Fiddler Capture of the accused instrumentality  Source: Fiddler Capture of the accused instrumentality
using the computer system to receive a second signal from an electronic device being used by the user, the second signal comprising a copy of the reusable identifier and user verification information;	The accused instrumentality practices using the computer system (e.g., authentication server of the accused instrumentality, etc.) to receive a second signal (e.g., a request signal from the user device) from an electronic device being used by the user, the second signal (e.g., request signal from the user device) comprising a copy of the reusable identifier (e.g., JSESSIONID, etc.) and user verification information (e.g., kampyle_userid). When the server sends a message containing an FPID to the user device, the client includes a copy of the JSESSIONID in all subsequent requests to the server, along with user

	verification information (e.g., kampyle_userid credentials). This allows the server to authenticate the client for the duration of the session and ensure secure communication between the client and server.  Source: Fiddler Capture of the accused instrumentality  Source: Fiddler capture of the accused instrumentality

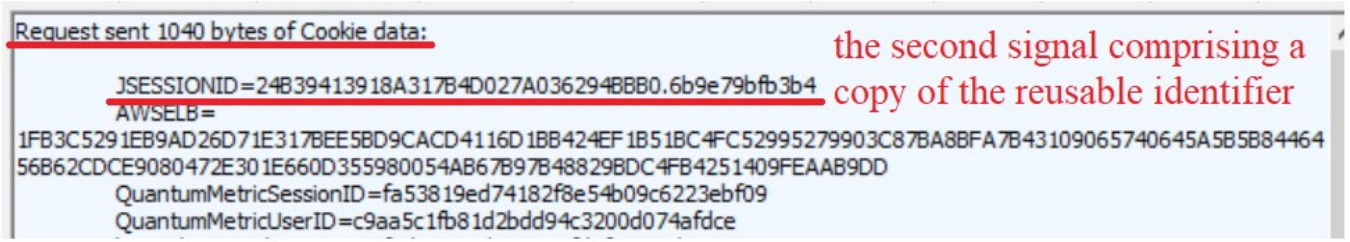
	 Source: Fiddler capture of the accused instrumentality
using a processor of the computer system to evaluate, based at least on the first signal and the second signal, whether the user is authorized to conduct the at least one interaction with the secured capability; and	The accused instrumentality practices using a processor of the computer system (e.g., processor of the authentication server of the accused instrumentality, etc.) to evaluate, based at least on the first signal (e.g., a JSESSIONID set response, etc.) and the second signal (e.g., a request signal from the user device), whether the user is authorized to conduct the at least one interaction (e.g., account login, etc.) with the secured capability (e.g., secure connection with the website, etc.). The server compares the reusable identifier, such as the token (e.g., JSESSIONID), in the first response received from the server with the token included in the client's subsequent request. If a match is found, the server authenticates the user and processes the request securely.



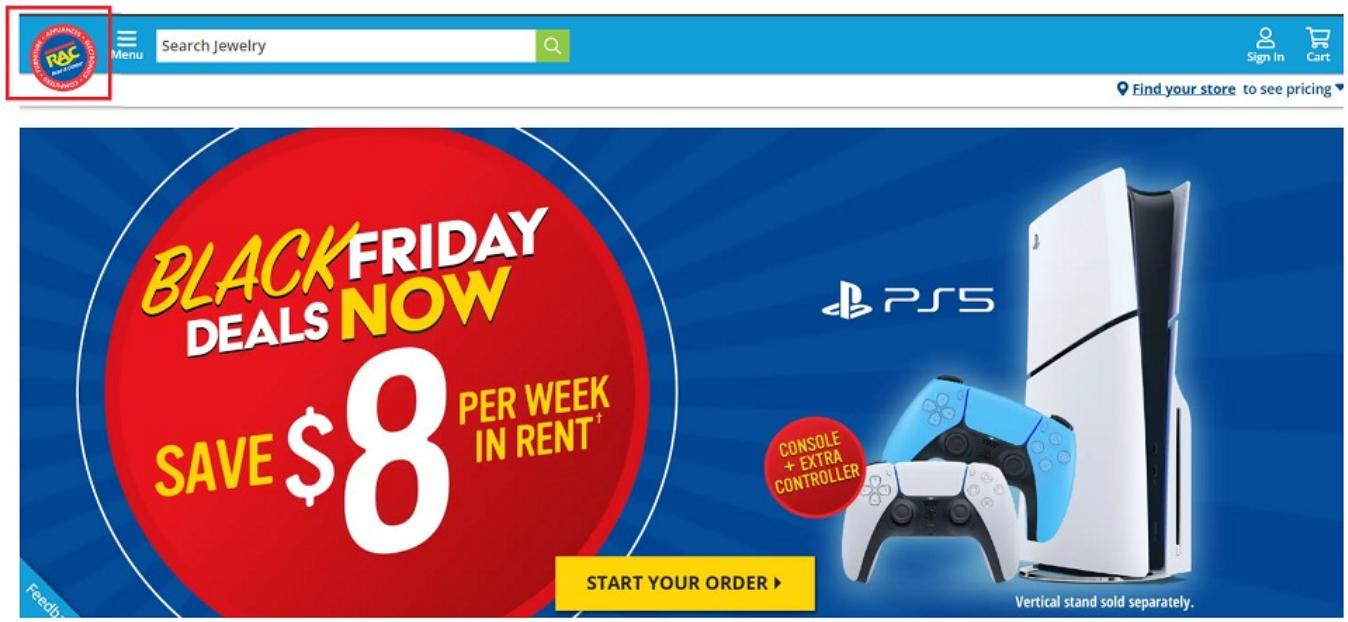
Source: Fiddler captures of the accused instrumentality



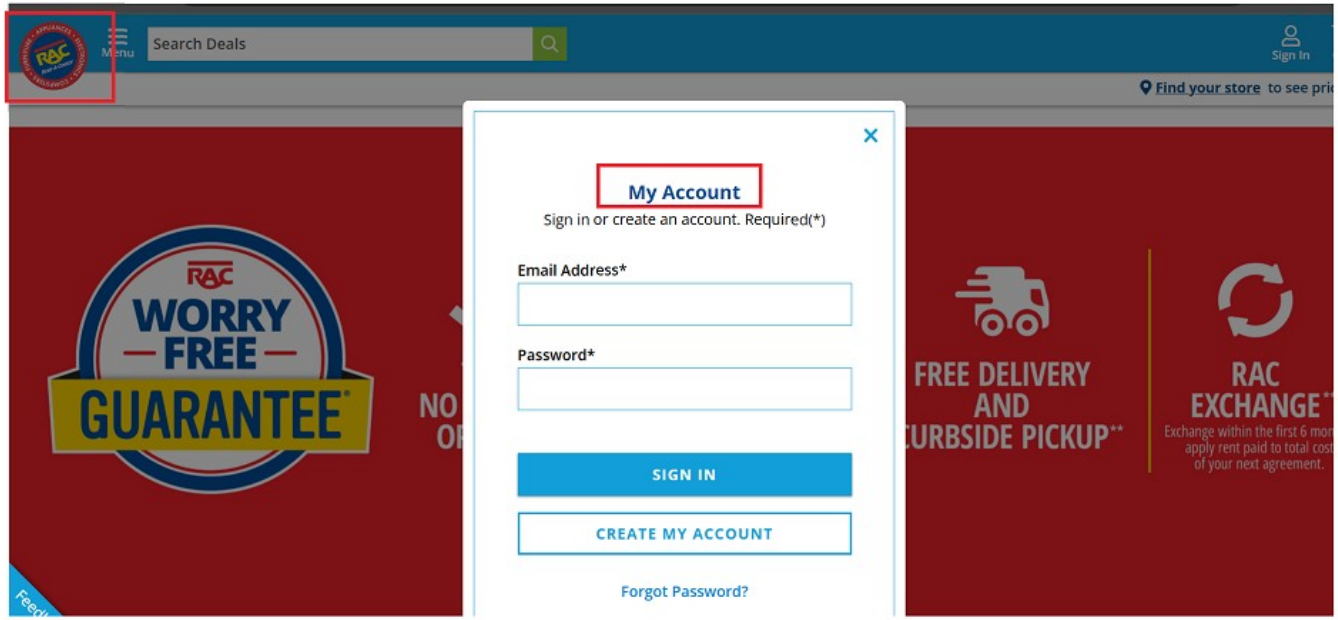
https://www.rentacenter.com/en/

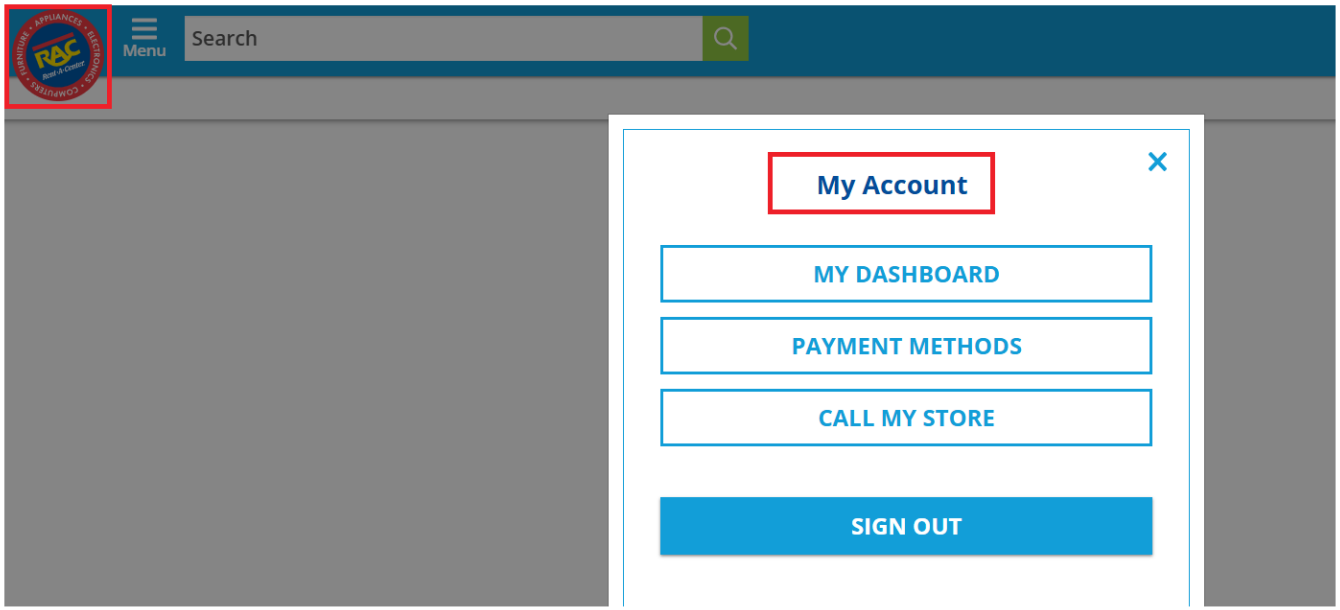


Source: Fiddler capture of the accused instrumentality

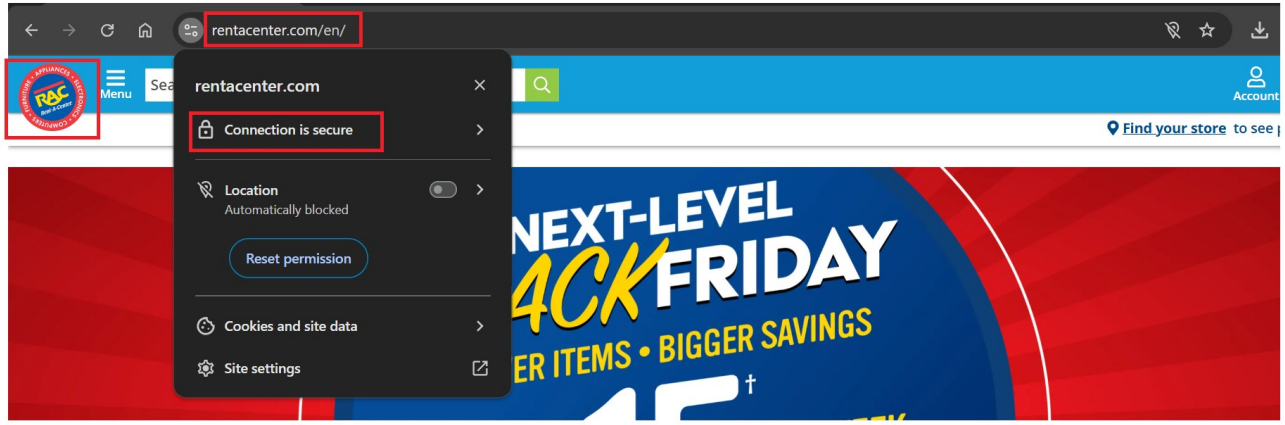


https://www.rentacenter.com/

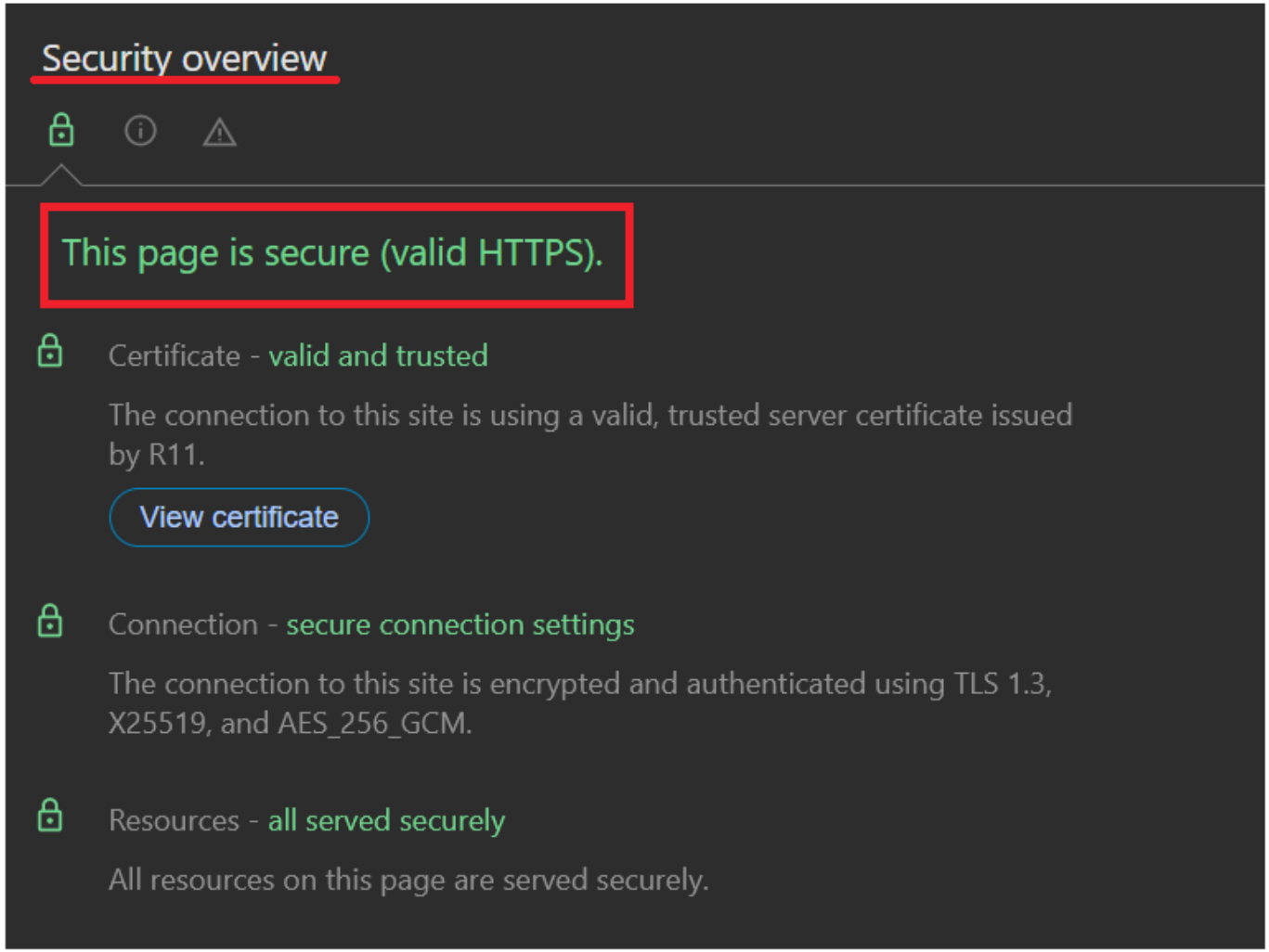
	 https://www.rentacenter.com/en/

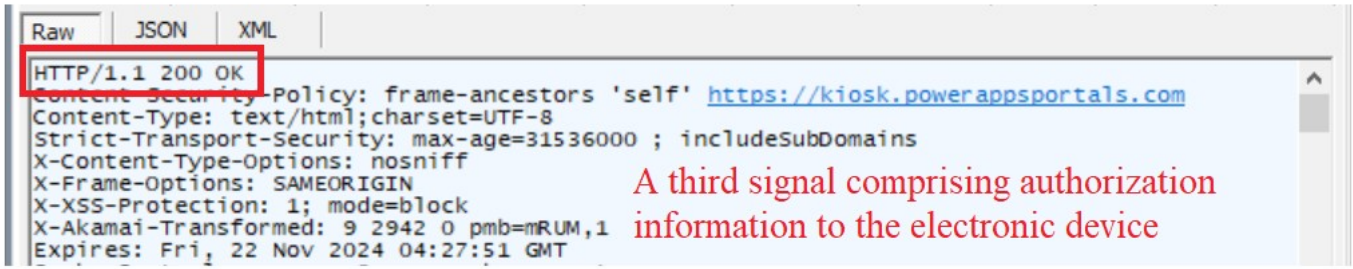


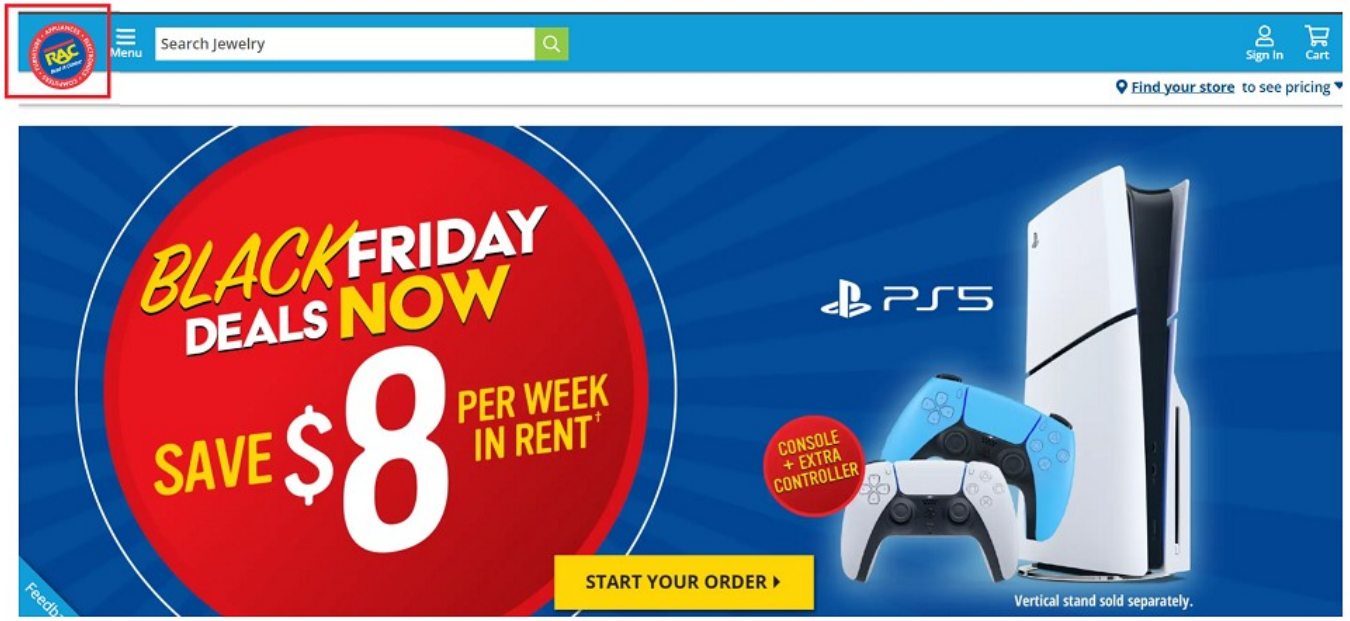
https://www.rentacenter.com/en/



https://www.rentacenter.com/en/

	 https://www.rentacenter.com/en/
in response to an indication	The accused instrumentality practices in response to an indication from the processor (e.g.,

from the processor that the user is authorized to conduct the at least one interaction with the secured capability, using the computer system to transmit a third signal comprising authorization information to at least one of the electronic device and the computer.	processor of the authentication server of the accused instrumentality, etc.) that the user is authorized to conduct the at least one interaction with the secured capability (e.g., secure connection with the website, etc.), using the computer system processor (e.g., authentication server of the accused instrumentality, etc.) to transmit a third signal comprising authorization information (e.g., a response signal from the server to the user device, etc.) to at least one of the electronic device (e.g., user device, etc.) and the computer. As shown, upon authenticating the JSESSIONID, the user device receives an authentication confirmation message (a third signal), from the server to the user device.  Source: Fiddler capture of the accused instrumentality

	 https://www.rentacenter.com/